



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/955,924	09/19/2001	Christian Huitema	212515	9394

23460 7590 12/21/2004

LEYDIG VOIT & MAYER, LTD
TWO PRUDENTIAL PLAZA, SUITE 4900
180 NORTH STETSON AVENUE
CHICAGO, IL 60601-6780

EXAMINER

CHAI, LONGBIT

ART UNIT PAPER NUMBER

2131

DATE MAILED: 12/21/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/955,924	HUITEMA ET AL.	
	Examiner	Art Unit	
	Longbit Chai	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on 28 May 2003.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☐ Claim(s) _____ is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-25 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 19 September 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date <u>5/28/2003</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. No claim for priority has been made in this application.

The effective filing date for the subject matter defined in the pending claims in this application is 9/19/2001.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

2. Claims 1, 3 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mooney (Patent Number: US 6351813 B1), hereinafter referred to as Mooney.

As per claim 1, Mooney teaches a method of forming a secure peer-to-peer group, comprising the steps of:

generating a group public/private key pair (Mooney: see for example, Column 9 Line 23 – 30 and Column 16 – 25);

defining group security properties (Mooney: see for example, Column 9 Line 23 – 30 and Column 16 – 25);

Mooney does not disclose expressly generating a group identification as a hash of the group public key.

However, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify Mooney to accommodate generating a group identification as a hash of the group public key because (a) Mooney discloses group public key (Mooney: see for example, Column 9 Line 23 – 30 and Column 16 – 25), (b) Mooney teaches the access code to the group resource (equivalent to the group identification number) is the hash of the group information containing at least a common answer of a question from each member in the group (Mooney: see for example, Column 17 Line 10 – 18) and (c) the group public key is well known in the art, which is one of the obvious choices to be qualified as a piece of information that is common to the entire group of the members as taught by Mooney.

As per claim 3, Mooney as modified teaches the claimed invention as described above (see claim 1). Mooney as modified further teaches generating a group shared key to be used to encrypt group traffic (Mooney: see for example, Column 9 Line 25 – 30).

As per claim 22, Mooney as modified teaches the claimed invention as described above (see claim 1). Mooney as modified further teaches computer-readable medium having computer-executable instructions (Mooney: see for example, Figure 1).

Art Unit: 2131

3. Claims 8, 9 and 23 – 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hanna (Patent Number: US 2002/0144149 A1), hereinafter referred to as Hanna.

As per claim 8, Hanna teaches in a secure peer-to-peer group having a predefined public/private key pair (P_G / K_G), a method of inviting a peer to join the group, comprising the steps of:

obtaining a public key (P_{U1}) of a peer (Hanna: see for example, Figure 6 Element 42 & Element 44 and Paragraph [0027] and [0030]);

forming a first group membership certificate containing the peer's public key (P_{U1}) and a second membership certificate signed with the group private key (K_G), the first group membership certificate being signed with a private key of an issuer (K_{U2}) (Hanna: see for example, Figure 6 Element 42 & Element 44 and Paragraph [0027] & Paragraph [0030]); and

sending the group membership certificate to the peer to invite the peer to join the group (Hanna: see for example, Paragraph [0024]).

Hanna does not disclose explicitly the method to invite the peer to join the group.

However, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify Hanna to accommodate inviting the peer to join the group because Hanna teaches the method for a user to request the access to a resource that belongs to a particular group which is obviously equivalent to request the participation (or join) to that particular group so that the access can be granted (Hanna:

Art Unit: 2131

see for example, Figure 6 Element 42 & Element 44 and Paragraph [0027] & Paragraph [0030]).

As per claim 9, Hanna teaches the claimed invention as described above (see claim 8). Hanna further teaches forming a group membership certificate comprises the step of forming a group membership certificate having a structure $((P_{U1}) K_G) K_{U2}$ (Hanna: see for example, Figure 6 Element 42 and Paragraph [0027] & Paragraph [0030]).

As per claim 23, 24 and 25, Hanna as modified teaches the claimed invention as described above (see claim 8, 13 and 18 respectively). Hanna as modified further teaches computer-readable medium having computer-executable instructions (Hanna: see for example, Paragraph [0049]).

4. Claims 10, 13, 14, 18 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hanna (Patent Number: US 2002/0144149 A1), hereinafter referred to as Hanna, in view of Mittra (Patent Number: 5748736), hereinafter referred to as Mittra.

As per claim 13, Hanna teaches a method of securely joining a peer-to-peer group by a peer having a public and a private key, comprising the steps of:

Art Unit: 2131

receiving a group invitation containing an invitation certificate having a group ID provided therein; resolving the group ID to find a member of the group (Hanna: see for example, Figure 6 and Paragraph [0028] Last 2nd Sentence);

sending a connect message to the member containing the invitation certificate signed with the private key (Hanna: see for example, Figure 6 Element 42 and Paragraph [0027] & Paragraph [0030]);

Hanna does not disclose expressly receiving a group shared key to enable decryption of group traffic. However, Hanna teaches that the access to the resource of the group should be granted as the result of group authentication process (Mooney: see for example, Paragraph [0028]), which is evidently that the group shared key should be given out to the user in order to access the encrypted / protected group data successfully.

Hanna does not disclose expressly receiving an accept message from the member containing a group membership certificate signed by a private key of the member.

Mittra teaches receiving an accept message from the member containing a group membership certificate signed by a private key of the member (Mittra: see for example, Column 14 Line 34 – 35).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Mittra within the system of Hanna because (a) Hanna teaches, specifically, a technique for verifying security membership in a group authorized to obtain access to a predetermined resource in a distributed

Art Unit: 2131

environment (Hanna: see for example, Paragraph [0003]) and (b) Mittra teaches an improved system and method for secure group communications (Mittra: see for example, Column 1 Line 50 – 55).

As per claim 14, Hanna as modified teaches the claimed invention as described above (see claim 13). Hanna as modified further teaches authenticating the group membership certificate signed by the private key of the member to ensure the member's association with the group (Mittra: see for example, Column 1 Line 50 – 55).

As per claim 18 and 20, claim 18 and 20 does not further teach over claim 13. Therefore, see same rationale addressed above in rejecting claim 13.

As per claim 10, claim 10 does not further teach over claim 18. Therefore, see same rationale addressed above in rejecting claim 18.

5. Claim 2, 5 and 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mooney (Patent Number: US 6351813 B1), hereinafter referred to as Mooney, in view of Hanna (Patent Number: US 2002/0144149 A1), hereinafter referred to as Hanna.

As per claim 2, Mooney as modified teaches the claimed invention as described above (see claim 1). Mooney as modified does not disclose expressly obtaining a public key of a peer, forming a group membership certificate containing the peer's public

Art Unit: 2131

key and signed with the group private key; and sending the group membership certificate to the peer to invite the peer to join the group.

Hanna teaches obtaining a public key of a peer; forming a group membership certificate containing the peer's public key and signed with the group private key; and sending the group membership certificate to the peer to invite the peer to join the group (Hanna: see for example, Figure 6 Element 42 & Element 44 and Paragraph [0027], [0030] and [0024]).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Hanna within the system of Mooney as modified because (a) Mooney as modified discloses the group security concept for various groups / classes of users (Mooney: see for example, Column 1 Line 54 – 56) and (b) Hanna teaches, specifically, a technique for verifying security membership in a group authorized to obtain access to a predetermined resource (Hanna: see for example, Paragraph [0003]).

Hanna does not disclose explicitly the method to invite the peer to join the group.

However, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify and accommodate inviting the peer to join the group because Hanna teaches the method for a user to request the access to a resource that belongs to a particular group which is obviously equivalent for the user to request the participation (or join) of the group of interest so that the user's access to the resource can be granted (Hanna: see for example, Figure 6 Element 42 & Element 44 and Paragraph [0027] & Paragraph [0030]).

As per claim 5, Mooney as modified teaches the claimed invention as described above (see claim 2). Mooney as modified further teaches receiving a connect message from the peer containing the group certificate signed by a private key pair of the peer's public key; authenticating the group certificate signed by the peer's private key; and when the step of authenticating is successful, sending an accept message to the peer, and sending the group shared key to the peer (Hanna: see for example, Figure 6 Element 42 and Paragraph [0027] & Paragraph [0030]).

As per claim 6, Mooney as modified teaches the claimed invention as described above (see claim 5). Mooney as modified further teaches verifying that a signature of the certificate is valid; verifying that the certificate has not expired; verifying that the hash of the peer's public key matches the peer identification; opportunistically verifying ownership of the certificate (Hanna: see for example, Figure 6 Element 42 and Paragraph [0027] & Paragraph [0030]) & (Mooney: see for example, Column 9 Line 12 – 16).

6. Claims 11 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hanna (Patent Number: US 2002/0144149 A1), hereinafter referred to as Hanna, in view of Turnbull (Patent Number: 6092201), hereinafter referred to as Turnbull.

As per claim 11, Hanna teaches the claimed invention as described above (see claim 10). Hanna further teaches verifying that a signature of the third certificate is valid; verifying that the third certificate has not expired; verifying that the hash of the peer's public key matches a peer identification; opportunistically verifying ownership of the third certificate (Hanna: see for example, Figure 6 Element 42 and Paragraph [0027] & Paragraph [0030]).

Hanna does not disclose expressly verifying that the third certificate has not expired.

Turnbull teaches verifying that the third certificate has not expired (Turnbull: see for example, Column 5 Line 57 – 57, Column 6 Line 2 – 4 and Column 8 Line 20 – 24).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Turnbull within the system of Hanna because (a) Hanna discloses group certificate revocation lists (Hanna: see for example, Paragraph [0029] Last 2nd Sentence) and (b) Turnbull further explores the details of the group certificate revocation lists for extending secure communication operations (Turnbull: see for example, Column 2 Line 59 – 62).

As per claim 12, Hanna teaches the claimed invention as described above (see claim 10). Hanna further teaches group certificate revocation lists (Hanna: see for example, Paragraph [0029] Last 2nd Sentence). However, Hanna does not disclose explicitly the detail functions of group certificate revocation lists.

Turnbull teaches the specific details of the group certificate revocation lists such as determining if the certificate is listed in a group certificate revocation list (GCRL); determining if any certificates in a chain of group membership certificates is listed in the GCRL; when any certificates in the chain is listed in the GCRL, determining if a date of revocation of the certificate in the chain is before a date of issue of the peer's certificate; and when the date of revocation is after the date of issuance, issuing a new group certificate to the peer (Turnbull: see for example, Column 5 Line 57 – 57, Column 6 Line 2 – 4 and Column 8 Line 20 – 24).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Turnbull within the system of Hanna because (a) Hanna discloses group certificate revocation lists (Hanna: see for example, Paragraph [0029] Last 2nd Sentence) and (b) Turnbull further explores the details of the group certificate revocation lists for extending secure communication operations (Turnbull: see for example, Column 2 Line 59 – 62).

7. Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Mooney (Patent Number: US 6351813 B1), hereinafter referred to as Mooney, in view of Hanna (Patent Number: US 2002/0144149 A1), hereinafter referred to as Hanna, and in view of Turnbull (Patent Number: 6092201), hereinafter referred to as Turnbull.

As per claim 7, Mooney as modified teaches the claimed invention as described above (see claim 5). Mooney as modified further teaches group certificate revocation

lists (Hanna: see for example, Paragraph [0029] Last 2nd Sentence). However, Mooney as modified does not disclose explicitly the detail functions of group certificate revocation lists.

Turnbull teaches the specific details of the group certificate revocation lists such as determining if the certificate is listed in a group certificate revocation list (GCRL); determining if any certificates in a chain of group membership certificates is listed in the GCRL; when any certificates in the chain is listed in the GCRL, determining if a date of revocation of the certificate in the chain is before a date of issue of the peer's certificate; and when the date of revocation is after the date of issuance, issuing a new group certificate to the peer (Turnbull: see for example, Column 5 Line 57 – 57, Column 6 Line 2 – 4 and Column 8 Line 20 – 24).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Turnbull within the system of Mooney as modified because (a) Mooney as modified discloses group certificate revocation lists (Hanna: see for example, Paragraph [0029] Last 2nd Sentence) and (b) Turnbull further explores the details of the group certificate revocation lists for extending secure communication operations (Turnbull: see for example, Column 2 Line 59 – 62).

8. Claim 15 and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hanna (Patent Number: US 2002/0144149 A1), hereinafter referred to as Hanna, in view of Mittra (Patent Number: 5748736), hereinafter referred to as Mittra, and in view of Badovinatz (Patent Number: 6016505), hereinafter referred to as Badovinatz.

As per claim 15, Hanna as modified teaches the claimed invention as described above (see claim 14). Hanna as modified does not disclose expressly resolving the group ID to find a second member of the group to which to connect when the step of authenticating the group membership certificate signed by the private key of the member fails.

Badovinatz teaches resolving the group ID to find a second member of the group to which to connect when the step of authenticating the group membership certificate signed by the private key of the member fails (Badovinatz: see for example, Column 6 Line 54 – 58: Badovinatz teaches the communication means within a group can be flexible enough so that any member and not fixed (or default) member can only communicate with a given user).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Badovinatz within the system of Hanna because (a) Hanna teaches, specifically, a technique for verifying security membership in a group authorized to obtain access to a predetermined resource in a distributed environment (Hanna: see for example, Paragraph [0003]) and (b) Badovinatz teaches providing Group Services in a highly-available systems (Badovinatz: see for example, Column 3 Line 58 – 64).

As per claim 17, claim 17 does not further teach over claim 13 and 15. Therefore, see same rationale addressed above in rejecting claim 13 and 15.

Art Unit: 2131

9. Claims 16, 19 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hanna (Patent Number: US 2002/0144149 A1), hereinafter referred to as Hanna, in view of Mittra (Patent Number: 5748736), hereinafter referred to as Mittra, and in view of Turnbull (Patent Number: 6092201), hereinafter referred to as Turnbull.

As per claim 16 and 19, Hanna as modified teaches the claimed invention as described above (see claim 14 and 18 respectively). Hanna as modified further teaches verifying that a signature of the certificate is valid; verifying that the certificate has not expired; verifying that the hash of the peer's public key matches the peer identification; opportunistically verifying ownership of the certificate (Hanna: see for example, Figure 6 Element 42 and Paragraph [0027] & Paragraph [0030]).

Hanna as modified does not disclose expressly verifying that the third certificate has not expired.

Turnbull teaches verifying that the third certificate has not expired (Turnbull: see for example, Column 5 Line 57 – 57, Column 6 Line 2 – 4 and Column 8 Line 20 – 24).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Turnbull within the system of Hanna as modified because (a) Hanna as modified discloses group certificate revocation lists (Hanna: see for example, Paragraph [0029] Last 2nd Sentence) and (b) Turnbull further explores the details of the group certificate revocation lists for extending secure communication operations (Turnbull: see for example, Column 2 Line 59 – 62).

As per claim 21, Hanna teaches the claimed invention as described above (see claim 20). Hanna as modified further teaches group certificate revocation lists (Hanna: see for example, Paragraph [0029] Last 2nd Sentence). However, Hanna as modified does not disclose explicitly the detail functions of group certificate revocation lists.

Turnbull teaches the specific details of the group certificate revocation lists such as determining if the certificate is listed in a group certificate revocation list (GCRL); determining if any certificates in a chain of group membership certificates is listed in the GCRL; when any certificates in the chain is listed in the GCRL, determining if a date of revocation of the certificate in the chain is before a date of issue of the peer's certificate; and when the date of revocation is after the date of issuance, issuing a new group certificate to the peer (Turnbull: see for example, Column 5 Line 57 – 57, Column 6 Line 2 – 4 and Column 8 Line 20 – 24).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Turnbull within the system of Hanna as modified because (a) Hanna as modified discloses group certificate revocation lists (Hanna: see for example, Paragraph [0029] Last 2nd Sentence) and (b) Turnbull further explores the details of the group certificate revocation lists for extending secure communication operations (Turnbull: see for example, Column 2 Line 59 – 62).

10. Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Mooney (Patent Number: US 6351813 B1), hereinafter referred to as Mooney, in view of Hanna

Art Unit: 2131

(Patent Number: US 2002/0144149 A1), hereinafter referred to as Hanna, and in view of Aucsmith (Patent Number: 5712914), hereinafter referred to as Aucsmith.

As per claim 4, Mooney as modified teaches the claimed invention as described above (see claim 2). Mooney as modified further teaches certificate comprises the step of forming a group membership certificate having a structure [Version, ID, Peer ID, Serial Number, Validity, Algorithms, P_{ID}, Pissuer] Kissuer (Mooney: see for example, Column 9) & (Hanna: see for example, Figure 6 Element 42 & Element 44 and Paragraph [0028] Last 2nd Sentence).

Mooney as modified does not disclose explicitly certificate Version ID and Serial Number.

Aucsmith teaches certificate Version ID and Serial Number (Aucsmith: see for example, Column 5 Line 1 – 39).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Aucsmith within the system of Mooney as modified because Aucsmith teaches the digital certificate conforming to recommendation X.509 for authentication (Aucsmith: see for example, Column 1 Line 10 – 11).

Art Unit: 2131

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788.


The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-3788.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Longbit Chai
Examiner
Art Unit 2131

LBC


Art Unit 2131
12/16/08